

**NOV 01 2007****PATENT**

Atty Docket No.: 100200290-1

**In The U.S. Patent and Trademark Office****In Re the Application of:**

**Inventor(s)** Zhichen XU et al. **Confirmation No.** 7480  
**Serial No.:** 10/084,499 **Examiner:** Jeffery L. Williams  
**Filed:** February 28, 2002 **Group Art Unit:** 2137  
**Title:** INCREASING PEER PRIVACY

**MAIL STOP APPEAL BRIEF - PATENTS**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**CERTIFICATE OF FACSIMILE TO THE USPTO**

I hereby certify that this correspondence is being transmitted to the Patent and Trademark Office facsimile number (571) 273-8300 on November 1, 2007. This correspondence contains the following document(s):


1 sheet of Transmittal of Reply Brief.

9 sheets of Reply Brief - Patents.

Respectfully submitted,

MANNAVA & KANG, P.C.

November 1, 2007

  
Ashok K. Mannava  
Reg. No.: 45,301

MANNAVA & KANG, P.C.  
8221 Old Courthouse Road  
Suite 104  
Vienna, VA 22182  
(703) 652-3822  
(703) 880-5270 (facsimile)

RECEIVED  
CENTRAL FAX CENTER

NOV 01 2007

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 100200290-1IN THE  
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Zhichen XU et al.

Confirmation No.: 7480

Application No.: 10/084,499

Examiner: Jeffery L. Williams

Filing Date: February 28, 2002

Group Art Unit: 2137

Title: INCREASING PEER PRIVACY

Mail Stop Appeal Brief - Patents  
Commissioner For Patents  
PO Box 1450  
Alexandria, VA 22313-1450TRANSMITTAL OF REPLY BRIEFTransmitted herewith is the Reply Brief with respect to the Examiner's Answer mailed on October 5, 2007.

This Reply Brief is being filed pursuant to 37 CFR 1.193(b) within two months of the date of the Examiner's Answer.

(Note: Extensions of time are not allowed under 37 CFR 1.136(a))

(Note: Failure to file a Reply Brief will result in dismissal of the Appeal as to the claims made subject to an expressly stated new ground rejection.)

No fee is required for filing of this Reply Brief.

If any fees are required please charge Deposit Account 08-2025.

- ☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450

Date of Deposit:

OR

- ☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571) 273-8300.  
Date of facsimile: November 1, 2007

Typed Name: Judy H. Chung

Signature: Judy H. Chung

Respectfully submitted,

Zhichen XU et al.

By Ashok K. Mannava

Ashok K. Mannava

Attorney/Agent for Applicant(s)

Reg No.: 45,301

Date: November 1, 2007

Telephone: (703) 652-3822

RECEIVED  
CENTRAL FAX CENTER

NOV 01 2007

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 100200290-1IN THE  
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Zhichen XU et al.

Confirmation No.: 7480

Application No.: 10/084,489

Examiner: Jeffery L. Williams

Filing Date: February 28, 2002

Group Art Unit: 2137

Title: INCREASING PEER PRIVACY

Mail Stop Appeal Brief - Patents  
Commissioner For Patents  
PO Box 1450  
Alexandria, VA 22313-1450

## TRANSMITTAL OF REPLY BRIEF

Transmitted herewith is the Reply Brief with respect to the Examiner's Answer mailed on October 5, 2007.

This Reply Brief is being filed pursuant to 37 CFR 1.193(b) within two months of the date of the Examiner's Answer.

(Note: Extensions of time are not allowed under 37 CFR 1.136(a))

(Note: Failure to file a Reply Brief will result in dismissal of the Appeal as to the claims made subject to an expressly stated new ground rejection.)

No fee is required for filing of this Reply Brief.

If any fees are required please charge Deposit Account 08-2025.

- ☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:  
Commissioner for Patents, Alexandria, VA 22313-1450  
Date of Deposit:

OR

- ☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (877) 273-8300.  
Date of facsimile: November 1, 2007

Typed Name: Judy H. Chung

Signature: Judy H. Chung

Respectfully submitted,

Zhichen XU et al.

By Ashok K. Mannava

Ashok K. Mannava

Attorney/Agent for Applicant(s)

Reg No.: 45,301

Date: November 1, 2007

Telephone: (703) 652-3822

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400

Attorney Docket No.: 100200290-1

RECEIVED  
CENTRAL FAX CENTER

NOV 01 2007

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**Inventor(s)** Zhichen XU et al. **Confirmation No.** 7480  
**Serial No.:** 10/084,499 **Examiner:** Jeffery L. Williams  
**Filed:** February 28, 2002 **Group Art Unit:** 2137  
**Title:** INCREASING PEER PRIVACY

**MAIL STOP APPEAL BRIEF - PATENTS**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**REPLY BRIEF - PATENTS**

Sir:

This reply brief is responsive to the Examiner's Answer mailed October 5, 2007.

**PATENT**

Atty Docket No.: 100200290-1  
App. Scr. No.: 10/084,499

**TABLE OF CONTENTS**

(1)	Objection to the Specification .....	3
(2)	Examiner's Arguments (i) Concerning 112 First Paragraph Rejection of Claim 42 (page 18 of the Examiner's Answer) .....	3
(3)	Examiner's Arguments (iii) Concerning Index Peers (page 20 of the Examiner's Answer) .....	4
(4)	Examiner's Arguments (ix) Concerning Encrypting a Transaction Identifier in Claim 21 (page 22 of the Examiner's Answer) .....	7
(5)	Conclusion .....	9

**PATENT**

Atty Docket No.: 100200290-1  
App. Ser. No.: 10/084,499

**(1) Objection to the Specification**

The Examiner's Answer indicates that the objection to the specification is not appealable. However, the objection forms the basis of the 112 first paragraph rejection. Accordingly, the Applicants request that the arguments in the Appeal Brief concerning the objection be considered for the 112 first paragraph rejection.

**(2) Examiner's Arguments (i) Concerning 112 First Paragraph Rejection of Claim 42 (page 18 of the Examiner's Answer)**

The Examiner argues that the specification does not support storing the received label upon the condition that any label stored in the table does not match the received label. Claim 42 recites,

if a label stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message, the intermediate peer stores the predetermined label and the corresponding identity of the next peer.

Claim 42 does not recite the condition, "if any stored label does not match, ... ." Instead, claim 42 recites if "a" label does not match, ... . Thus, the condition of if the predetermined label is not present in the table, which is disclosed in the specification, provides support for the claimed condition of if a label does not match.

**PATENT**

Atty Docket No.: 100200290-1  
App. Ser. No.: 10/084,499

**(3) Examiner's Arguments (iii) Concerning Index Peers (page 20 of the Examiner's Answer)**

On page 20 of the Examiner's Answer, in sections (iii), the Examiner argues that every peer in the path in Goldschlag is an index peer, and the index peers are indexed in a table stored on each of the peers in the path. See Goldschlag; p.5, par. 1; p. 10, par. 3.

Even given this new interpretation of Goldschlag, Goldschlag fails to teach the features of claim 1.

A short description of Goldschlag is as follows, and then an indication of the claimed features not taught is provided. In section 3.1 on page 6 of Goldschlag, Goldschlag discloses creating virtual circuits between routing nodes in a path. This is done by sending an onion, such as shown in figure 2. A message is created which includes the onion and a header. The header includes a circuit identifier and the "create" command. Each node that receives the onion, peels a layer off the onion to determine the next node. Also, each node stores in a table the received circuit identifier and a new circuit identifier chosen by the node, along with forward and backward cryptographic function/key pairs. The received circuit identifier is later used to search the table to identify the circuit identifier (previously chosen by the node) for sending to the next node and for identifying the appropriate function/key pair. Figure 3 shows an example of a virtual circuit created using the onion, which includes nodes W, X, Y and Z.

After the virtual circuit is created, data may be sent along the virtual circuit using a "data" command. The "data" command is described in Goldschlag on page 11, first full paragraph. For example, the initiator node pre-crypts data in layers using the forward

**PATENT**

Atty Docket No.: 100200290-1

App. Ser. No.: 10/084,499

function/key encryption pairs for each node in the path of the virtual circuit. The inner most layer of the pre-crypted data is encrypted with the responder's (c.g., node Z shown in figure 3) forward function/key pair, and the next higher layer is pre-crypted with the forward function/key pair of the node (c.g., node Y) next to the responder, and so on. The pre-crypted data with all the layers is sent in a message from the initiator to the next node in the path (e.g., node X). The message also includes the "label", i.e., the virtual circuit identifier, previously sent to node X with the "create" onion. Node X uses the label to perform a lookup to determine the virtual circuit identifier previously chosen by the node X, which is used to send the "data" onion to Node Y. The lookup also identifies the forward function/key pair for the virtual circuit. The forward function/key pair is used to peel (i.e., decrypt) a layer from the "data" onion, and the retrieved virtual circuit identifier is used to send the peeled, "data" onion to the next node, which is Node Y.

Given the interpretation that all the nodes in the path are index nodes, Goldschlag still fails to teach the following features of claim 1:

determining a next peer according to said path for said information by searching said table of each peer of said plurality of peers with said path index as an index into said table;

retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer;

encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index; and



**PATENT**

Atty Docket No.: 100200290-1  
App. Ser. No.: 10/084,499

transmitting a new message with said information and said next state of said path index as said path index to said next peer.

When the virtual circuit is created using the "create" command, Goldschlag does not determine a next peer by searching a table using the path index. Instead, the next node is determined by decrypting the layer using its public key. See figure 2 and page 5, line 2. When data is sent in an onion using the "data" command, the received virtual circuit identifier is used to perform a lookup in the receiving node table to determine the corresponding stored virtual circuit identifier identifying the next node. However, claim 1 recites encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index. Goldschlag does not disclose this stored virtual circuit identifier is encrypted. When the "data" onion is pre-encrypted by the initiator, it knows the forward function/key pairs for the nodes in the path. However, the initiator does know the virtual circuit identifiers chosen by each of the nodes in the path. Thus, this information is not encrypted, and is instead included in the header of the message sent to the next node by each node receiving the "data" onion. Furthermore, if the message, including the header, were encrypted, it could only be encrypted with the public key of the next node, and not the public key of a respective index node or another node in the path, because the receiving node (e.g., Node X) only knows the next node in the path (e.g., Node Y). The identities of all the other nodes in the path are concealed by the onion, such as shown in figure 2, when the virtual circuit is created.

**PATENT**

Atty Docket No.: 100200290-1

App. Scr. No.: 10/084,499

Again, taking the interpretation of the Examiner that all the nodes in the path are index nodes, the steps of

(1) retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer, and

(2) encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index

would require a node in Goldschlag to retrieve the identity of a next node and another node in the path, and then encrypt an index with the public key of the another node in the path. However, a node in Goldschlag only knows the next node. The identity of the other nodes is concealed in the onion. Also, this interpretation would require encrypting the virtual circuit identifier (the path index) chosen by the node with the public key of a node in the path which is not the next node. As described above, Goldschlag fails to teach the virtual circuit identifier is encrypted. Also, the public key of a node that is not the next node is not known, so it cannot be used to encrypt the virtual circuit identifier.

**(4) Examiner's Arguments (ix) Concerning Encrypting a Transaction Identifier in Claim 21 (page 22 of the Examiner's Answer)**

The Examiner argues that expiration time identifies a valid transaction and thus is an identifier of a transaction. The Examiner further argues that the specification discloses the transaction identifier as a value, and the expiration time is a value. The Examiner, however, disregards the disclosure in the specification that the value is used to identify the requested

**PATENT**

Atty Docket No.: 100200290-1  
App. Ser. No.: 10/084,499

information. For example, the identifier is later used to by the peer privacy module to identify the requested information for the setup message.

The expiration time of Goldschlag is a time. Specifically, it identifies a time when an onion expires. It does not identify a transaction, a message or requested information. It may be used to determine whether an onion is valid. However, it does not specifically identify whether an onion is valid. Thus, it does not identify a "valid" transaction as alleged by the Examiner

**PATENT**

Atty Docket No.: 100200290-1

App. Ser. No.: 10/084,499

**(5) Conclusion**

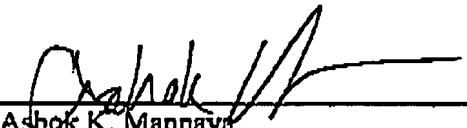
For at least the reasons given above, the rejection of claims 1, 3-20, and 22-29 is improper. Accordingly, it is respectfully requested that such a rejection by the examiner be reversed and these claims be allowed. Attached below for the Board's convenience is an Appendix of claims 1, 3-20, and 22-29 as currently pending and on appeal.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: November 1, 2007

By

  
Ashok K. Mannava  
Registration No.: 45,301

MANNAVA & KANG, P.C.  
8221 Old Courthouse Road  
Suite 104  
Vienna, VA 22182  
(703) 652-3822  
(703) 865-5150 (facsimile)